UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/385,591	08/29/1999	GARY L. GRAUNKE	42390.P7573	9395

7590 12/23/2004

ALOYSIUS T C AUYEUNG
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
7TH FLOOR
12400 WILSHIRE BOULEVARD
LOS ANGELES, CA 90025

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/385,591	GRAUNKE ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *28-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 28-47 have been examined. The Applicant in the amendment filed on November 8, 2004 amended claims 28, 31, 36, 38, 39, 40, 42 and 46. Claims 1-27 were canceled in a previous amendment.

Response to Amendment

2. The objection to the title is withdrawn as the amended title is more clearly indicative of the claimed invention.

3. The objections to claims 38 and 40 are withdrawn as the amendments to the claims overcome the objections.

4. The 35 U.S.C. 112, 2nd paragraph rejections to claims 31, 36, 42, and 46 are withdrawn as the amendments to the claims overcome the 112, 2nd paragraph rejections.

Response to Arguments

5. The following is a response to Applicant's arguments listed on pages 7-14 in the amendment filed on November 9, 2004.

6. Applicant's argument that "Feistel does not show, teach, use, or describe **a str am cipher key section** coupled with the block cipher key section **to modify the block cipher key**" (see pages 11-13, esp. page 11, 1st paragraph), have been fully

considered and are persuasive. As disclosed in Feistel, the stream cipher key section and block cipher key section are clearly coupled: in fact, all main components of the two sections are shared (see Feistel, Figures 2A and 2B; col. 10, line 43-col. 14, line 39), but, Feistel does not teach the stream cipher key section modifying the block cipher key according to a stream cipher key. Therefore, the 102 and 103 rejections to claims 28-47 has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Feistel modified by Schneier.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 28 and 39 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

9. Regarding claims 28 and 39, the phrases "(a transformed block cipher key)", (a modified random number)" in claim 28, and "(a selectively modified cipher key)", "(a transformed selectively modified cipher key)" and "(a transformed data bit sequence)" in claim 39 render the claims indefinite because it is unclear whether the limitations listed in parenthesis are part of the claimed invention. See MPEP § 2173.05(d). The following amendment is suggested: in claim 28, replace "(a transformed block cipher key)" with "into a transformed block cipher key" and "(a modified random number)" with "into a modified random number"; and in claim 39, replace "(a selectively modified

cipher key)" with "into a selectively modified cipher key", "(a transformed selectively modified cipher key)" with "into a transformed selectively modified cipher key", and "(a transformed data bit sequence)" with "into a transformed data bit sequence".

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 28, 32, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feistel U.S. Patent No. 4,316,055 (hereinafter Feistel 4,316,055) in view of Schneier Applied Cryptography 2nd Edition (hereinafter Schneier).

12. As per claim 28, Feistel 4,316,055 discloses a combination block/stream encoding apparatus (see Feistel 4,316,055; Title, Abstract) comprising:

a. a block cipher key section to be initialized with a block cipher key, having transformation units to transform the block cipher key (see Feistel 4,316,055; col. 5, lines 34-40; Figure 4, Reference Nos. 9, 10, 12, 13 and related text);

b. a data section coupled with the block cipher key section to be initialized with a random number, having transformation units to transform the random

number based on the transformed block cipher key (see Feistel 4,316,055; Figure 1, MSR and Transformation Element);

c. a stream cipher key section coupled with the block cipher key section to produce data bits to dynamically modify the random number in the data block section (see Feistel 4,316,055; col. 5, lines 31-40; Figure 2A, Reference Nos. 8 and 10, and related text; Figure 3, Reference No. 3 and related text; Figure 4, Reference Nos. 10-13 and related text); and

d. a mapping section to receive the modified random number and the transformed block cipher key and generate a pseudo random bit sequence based on the modified random number and the transformed block cipher key (see Feistel 4,316,055; Figure 2a, Reference Nos. 5, 20, 21; Figure 2b, Reference Nos. 22, 23, 24, 25, 26 MSR; Figure 4, Reference Nos. 12-13).

13. Feistel does not expressly teach the stream cipher key section modifying the block cipher key according to a stream cipher key to produce data bits. Schneier teaches an OFM block cipher wherein the block cipher key is modified by values from a shift register, and the modified block cipher key dynamically modifies the value in the data block section. See Schneier, pages 203-205, section 9.8. Moreover, since the stream cipher key and the block cipher key are one and the same in Feistel (see Feistel, Figure 2a, Reference No. 3), and the values of the shift register in Schneier come from the modified key value derived from the block cipher key, the invention of Feistel modified by Schneier covers a stream cipher key section modifying the block cipher key according to a stream cipher key. It would be obvious to one of ordinary skill in the art

at the time the invention was made to modify the invention of Feistel with the teaching of Schneier wherein the stream cipher key section modifying the block cipher key according to a stream cipher key to produce data bits to dynamically modify the random number in the data block section. Motivation to combine includes, inter alia, randomizing the block cipher key for a more secure cipher system. See Schneier, page 209, "OFG/Counter: Security". The aforementioned cover the limitations of claim 28.

14. As per claims 32 and 33, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). In addition, the data section is initialized with either plain text or a derived random number. See Feistel 4,316,055; col. 12, line 33-col. 13, line 14; col. 10, line 42-col. 11, line 2. The aforementioned cover the limitations of claims 32 and 33.

15. Claims 29-31, 34-37, 39, and 41-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feistel 4,316,055 in view of Feistel US. Patent No. 3,798,360 (hereinafter Feistel 3,798,360).

16. As per claims 34-36, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Feistel 4,316,055 does not disclose the data section to further include fourth, fifth, and sixth registers wherein substitution units are coupled to an output of the fourth register and an input of the sixth register and linear transformation units are coupled between an

output of the fifth register and an input of the fourth register and an output of the sixth register and an input of the fifth register. However, a step code ciphering system found in Feistel 3,798,360 largely covers these limitations regarding a fourth, fifth, and sixth blocks with the above substitution and transformation relations. See Feistel 3,798,360; Figure 1, Reference Nos. 20, 22, 28, Steps 1, 2, 3, 4, 5, 6 and related text; Figures 3a-c and related text, especially 'MANGLER' and 'CONFUSER'. Furthermore, since Feistel 3,798,360 teaches that the segmentation of the data blocks are a matter of design choice (see Feistel 3,798,360; col. 3, lines 19-24; col. 4, lines 65-68), the fourth, fifth, and sixth blocks are operatively functional as fourth, fifth, and sixth registers. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the apparatus of Feistel 3,798,360 to the data section of Feistel 4,316,055. Motivation to combine enables an efficient and secure ciphering means using substitution and transformation steps as taught by Feistel 3,798,360. Ibid. The aforementioned cover the limitations claims 34-36.

17. As per claims 29-31, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Feistel 4,316,055 does not disclose the block cipher key section including first, second, and third registers wherein substitution units are coupled to an output of the first register and an input of the third register and linear transformation units are coupled between an output of the second register and an input of the first register and an output of the third register and an input of the second register. However, it is notoriously well known in the

art for cipher keys to be generated by a cryptographic cipher (devices that are aptly named pseudo-random number generators) since cryptographic ciphers create essentially random strings from non-random strings for encryption purposes. Examiner takes Official Notice that cipher keys are conventionally generated using cryptographic means. Furthermore, the limitations claimed in claims 29-31 are based on cipher means in a key section that are operatively identical to the cipher means in the data section outlined in the claim 34-36 rejections listed above wherein the first, second, and third registers correspond to the fourth, fifth, and sixth registers respectively. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teachings of Feistel 3,798,360 as outlined in the claim 34-36 rejections above to the key section of the invention covered by Feistel 4,316,055. Motivation to combine enables means to create cryptographically secure cipher keys as known to one of ordinary skill in the art. The aforementioned cover the limitations of claims 29-31.

18. As per claim 37, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 29-31 and 34-36 rejections under 35 U.S.C. 103(a). In addition, the mapping section comprises a plurality of logical gates coupled with a register in the block cipher key section and a register in the data section. See Feistel 4,316, 055; Figures 2A, 2B as modified by Feistel 3,798,360; Figure 1, 'ENCIPHER'; see claim rejections 29-31. The aforementioned cover the limitations of claim 37.

19. As per claim 39, Feistel 4,316,055 covers a combination block/stream apparatus as outlined above in the claim 29-37 rejections under 35 U.S.C. 103(a). In addition, the second key section and the first key section are operatively equivalent to the block cipher key section and the stream cipher key section respectively. Feistel 4,316,055 also teaches the first key section is enabled in a stream cipher mode and disabled in a block cipher mode. See Feistel 4,316,055; Figure 2a, Reference No. 5; Figure 3, Reference No. 2 and related text. The aforementioned cover the limitations of claim 39.

20. As per claims 41-47, they are apparatus claims corresponding to claims 28-37 and 39, and they do not teach or define above the information claimed in claims 28-37 and 39. Therefore, claims 41-47 are rejected as being unpatentable over Feistel 4,316,055 in view of Feistel 3,798,360 for the same reasons set forth in the rejections of claims 28-37 and 39.

21. Claims 38 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feistel 4,316,055 in view of Coulthart et al. U.S. Patent No. 4,641,102 (hereinafter Coulthart).

22. As per claim 38, Feistel 4,316,055 covers a combination block/stream encoding apparatus as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Feistel 4,316,055 is silent on the matter of the stream cipher key section further including LFSRs to generate a first, second, and third sequence of bits wherein the third

sequence of data bits are shuffled using the first sequence of data and input bits and the second sequence of data and control bits. However, as specified in the claim 29-31 rejections, pseudo-random number generators are conventional means to create cryptographically secure keys. In addition, Coulthart discloses an unbiased random number generator having at least a first, second and third sequence of bits with the above mentioned shuffling units and relations using an LFSR. See Coulthart, Abstract, Figure 1. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement the random number generator as taught by Coulthart in the stream cipher key section of the invention covered by Feistel 4,316,055. Motivation to combine implements a cryptographically secure means to create cipher keys having a truer random value result as taught by Coulthart. Ibid. The aforementioned cover the limitations of claim 38.

23. As per claim 40, it is an apparatus claim corresponding to claims 38-39 and it does not teach or define above the information claimed in claims 38-39. Therefore, claim 40 is rejected as being unpatentable over Feistel 4,316,055 in view of Feistel 3,798,360 and Coulthart for the same reasons set forth in the rejections of claims 38-39.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
December 14, 2004

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100